AFRL-SR-AR-TR-09-0068

REPORT DOCUMENTATION PAGE

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
09-1-2008	Final	01/1/2005 to 6/30/08

4. TITLE AND SUBTITLE
Reasoning about Authorization and Security:

5a. CONTRACT NUMBER
FA9550-05-1-0055

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Joseph Y Halpern

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Cornell University, Ithaca, NY 14853

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NL
875 N. Randolph Street
Arlington, VA 22203
Dr Robert Herklotz

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This project had three main thrusts: (1) to create a language for expressing authorization policies that satisfied numerous desiderata, including being expressive, being easy to use, having precise semantics, and allowing for accountability; (2) to add the ability to express knowledgebased specifications to Nuprl, a well-developed language that has been used extensively to prove that programs satisfy their specifications, with the intent of then using Nuprl to automatically synthesize security protocols satisfying appropriate specifications; (3) to understand the extent to which it is possible to achieve robust security in the prseence of rational adversaries. With regard to (1), a language Lithium has been developed (jointly with Vicky Weissman) that satisfies many of the desiderata. Lithium was chosen as the language for NRL's MLWeb project.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*

Reasoning about Authorization and Security: Final Report

Joseph Y. Halpern

Grant No: AFOSR FA9550-05-1-0055
PI: Joseph Y. Halpern
Institution: Cornell University, Ithaca, NY 14853

Executive Summary

This project had three main thrusts: (1) to create a language for expressing authorization policies that satisfied numerous desiderata, including being expressive, being easy to use, having precise semantics, and allowing for accountability; (2) to add the ability to express knowledge-based specifications to Nuprl, a well-developed language that has been used extensively to prove that programs satisfy their specifications, with the intent of then using Nuprl to automatically synthesize security protocols satisfying appropriate specifications; (3) to understand the extent to which it is possible to achieve robust security in the prseence of rational adversaries. With regard to (1), a language Lithium has been developed (jointly with Vicky Weissman) that satisfies many of the desiderata. Lithium was chosen as the language for NRL's MLWeb project. Halpern and Weissman worked with NRL to implement it. Due to funding problems, they implemented only part of the language. In addition, Weissman's work on giving semantics to ODRL (Open Digital Rights Language—see http://odrl.net) led to her being invited to serve on the ODRL working group, charged with giving semantics to the next version of ODRL. Weissman received her Ph.D., which was largely based on this work, in 2007. With regard to (2), working with Sabina Petride, Mark Bickford, and Robert Constable, we have added the ability to express knowledge-based specifications in Nuprl, and shown that in can be used to capture a number of specifications of interest. Petride has completed her B exam and is about to submit her Ph.D. thesis, the thesis includes a major section on using knowledge-based specifications in Nuprl. Finally, with regard to (3), working with Danny Dolev and Ittai Abraham, we have combined ideas from fault tolerance, game theory, and cryptography to design algorithms that guarantee robust security in the face of rational adversaries (that is, adversaries who have well-understood payoffs, who can be incentivized appropriately), while allowing a certain fraction of the adversaries to behave in completely unpredictable ways, and proving that these algorithms are optimal, by proving matching lower bounds. All this work has led to numerous publications and invited talks.

20090324165

Objectives

Originally, this project had two goals. The first was to find a language for expressing authorization policies that satisfies the following desiderata:

(a) it is expressive (so that all policies of interest can be expressed);

(b) it is tractable (so that it is easy to to compute what is permitted by a collection of policies);

(c) it is unambiguous (so that there's no ambiguity about what a policy means);

(d) it is easy for intelligent nonexperts to use;

(e) it supports accountability (so that it is easy to understand which policies lead to a particular permission and who made these policies);

(f) it allows for easy comparison of policy sets (for example, it allows us to ascertain whether one policy set is more permissive than another or whether two policy sets are in some sense equivalent);

(g) it supports policy management (for example, it allows merging two sets of policies, or dynamically updating policies over time in an easy way).

(h) it has the support of industry (so that companies are willing to create products that "understand" and enforce policies written in the language).

The second goal was to add the ability to express knowledge-based specifications in Nuprl, a well-developed language that has been used extensively to prove that programs satisfy their specifications, with the intent of then using Nuprl to automatically synthesize security protocols satisfying appropriate specifications.

Recently, a third focus of the project has been to achieve robust security in the presence of rational adversaries.

Status

Vicky Weissman and I completed our work with NRL on MLWeb; they implemented part of the language, but not all of it, due to lack of funding. Sabina Petride has completed her B exam and should hand in her thesis in the next few weeks; the thesis includes a major section on using knowledge-based specifications in Nuprl. Finally, Ittai Abraham, Danny Dolev, and I have precisely characterized the conditions under which it is possible to achieve fault tolerance in a game-theoretic setting in synchronous systems; we are currently working on extending these results to asynchronous systems.

Accomplishments

Ittai Abraham, Danny Dolev, and I have precisely characterized the conditions under which it is possible to achieve fault tolerance in a game-theoretic setting in synchronous systems; we are currently working on extending these results to asynchronous systems. As a spinoff of these results, we were able to obtain the best-known results on achieving Byzantine agreement in asynchronous systems, showing that it can be done with probability 1, in polynomial time, as long as fewer than one-third of the processes are faulty. (It was known that it could not be done if more than one-third of the processes are faulty.) Sabina Petride, Mark Bickford, Robert Constable, and I have just about finished a paper reporting our results on knowledge-based specifications in Nuprl. This will form part of Sabina's thesis, which should be handed in during this reporting period.

Personnel Supported

Joseph Halpern (PI), Sucheta Soundarajaan (graduate student), Danny Dolev (visitor), Victoria Weissman (former graduate student).

Publications (October 1, 2007 - September 30, 2008)

1. J. Y. Halpern and R. Pucella, Characterizing and reasoning about probabilistic and non-probabilistic expectation, *Journal of the ACM* **54**:3, 2007.

2. J. Y. Halpern and L. C. Rego, Characterizing the NP-PSPACE gap in the satisfiability problem for modal logic, *Journal of Logic and Computation* **17**:4, pp. 795-806, 2007.

3. F. C. Chu and J. Y. Halpern, Great expectations. Part I: On the customizability of generalized expected utility, *Theory and Decision* **64**:1, 2008, pp. 1-36

4. J. Y. Halpern and L. C. Rego, Interactive unawareness revisited, *Games and Economic Behavior* **62**:1, 2008, pp. 232–262.

5. J. Y. Halpern and V. Weissman, A formal foundation for XrML, *Journal of the ACM* **55**:1, 2008.

6. H. Chockler, J. Y. Halpern, and O. Kupferman, What causes a system to satisfy a specification?, *ACM Transactions on Computational Logic* **9**:3, 2008.

7. D. J. Martin, J. Gehrke, and J. Y. Halpern, Toward expressive and scalable sponsored search auctions, *Proc. 24th International Conference on Data Engineering*, 2008, pp. 237-246.

8. I. Abraham, D. Dolev, and J. Y. Halpern, Lower bounds on implementing robust and resilient mediators, *Proc. Fifth Theory of Cryptography Conference*, 2008, pp. 302-319.

9. J. Y. Halpern, From qualitative to quantitative proofs of security properties using first-order conditional logic, *AAAI-08 (Proceedings of the Twenty-Third AAAI Conference on Artificial Intelligence)*, 2008, pp. 459–464.

10. I. Abraham, D. Dolev, and J. Y. Halpern, An almost-surely terminating polynomial protocol for asynchronous Byzantine agreement with optimal resilience, *Procedings of the Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing*, 2008, pp. 405–414.

11. I. Kash, E. J. Friedman, and J. Y. Halpern, The Lotus-eater attack, *Procedings of the Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing*, 2008, p. 455.

12. J. Y. Halpern, Beyond Nash equilibrium: solution concepts for the 21st century, *Proceedings of Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing*, 2008, pp. 1–10. Reprinted in *Proceedings of the Eleventh International Conference on Principles of Knowledge Representation and Reasoning (KR 2008)*, 2008.

13. J. Y. Halpern, Computer science and game theory: A brief survey, *The New Palgrave Dictionary of Economics*, (S. N. Durlauf and L. E. Blume, eds.) Palgrave MacMillan, 2008.

14. P. D. Grünwald and J. Y. Halpern, A game-theoretic analysis of updating sets of probabilities, *Proceedings of the Twenty-Fourth Conference on Uncertainty in AI*, 2008, pp. 240–247.

15. J. Y. Halpern, Defaults and normality in causal structures, *Proceedings of the Eleventh International Conference on Principles of Knowledge Representation and Reasoning (KR 2008)*, 2008.

16. J. Y. Halpern, Joseph Y. Halpern, in *Epistemology: 5 Questions* (ed. V. F Hendricks and D. Pritchard), Automatic Press/VIP, 2008, pp. 155–166.

Participation/Interactions

Joseph Halpern gave the following talks:

- Distributed Computing Meets Game Theory: Robust Mechanisms for Rational Secret Sharing and Multiparty Computation,
  - ETH, Zurich (June, 2008)
- Redoing the foundations of decision theory
  - University of Kentucky, Computer Science Colloquium (January, 2008)
  - University of Indiana, Cognitive Science Colloquium (March, 2008)
- Constructive Decision Theory
  - Invited talk, Cowles Conference on Choice, Contracts, and Computation, New Haven (June 2008)
  - Invited talk, Workshop on Bayes and Savage, Bergen, Norway (June, 2008)

- University of Queensland, Australia, Economics Dept. Colloquium (Sept., 2008)

- Causality, responsibility, and blame: a structural-model approach,
  - University of Indiana, Computer Science Colloquium (March, 2008)

- Beyond Nash equilibrium: Solution concepts for the 21st Century
  - EPFL, Lausanne, Switzerland (June, 2008)
  - Invited talk, Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing, Toronto (August, 2008)
  - Invited talk, Eleventh International Conference on Principles of Knowledge Representation and Reasoning (KR 2008), Sydney, Australia (September, 2008).

- Reasoning About Knowledge in Multiagent Systems
  - Invited talk, Workshop on Information, Control, and Communication, Berlin (April, 2008)

- From qualitative to quantitative proofs of security properties using first-order conditional logic
  - AAAI-08 (Twenty-Third AAAI Conference on Artificial Intelligence), Chicago (June, 2008)

- An almost-surely terminating polynomial protocol for asynchronous Byzantine agreement with optimal resilience
  - Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing, Toronto (August, 2008)

- Defaults and normality in causal structures
  - Eleventh International Conference on Principles of Knowledge Representation and Reasoning (KR 2008), Sydney, Australia (Sept., 2008).

Consultative and advisory functions

None this year.

New discoveries, inventions or patent disclosures

- D. J. Martin, J. Y. Halpern, and J. Gehrke, System and Method for Scalable Sponsored Auctions, patent application filed August, 2008.

Honors/Awards

- Selected Fellow of AAAS, November, 2005.
- Selected Fellow of ACM, 2002.
- Fulbright Fellow, 2001-02.
- Guggenheim Fellow, 2001-02.
- Milner Lecturer, University of Edinburgh, 2000.
- Awarded 1997 Gödel Prize for outstanding paper in the area of theoretical computer science for "Knowledge and common knowledge in a distributed environment".
- Fellow of the American Association of Artificial Intelligence, 1993.